LISTING OF CLAIMS

1. (currently amended) A method for securely providing data of a content provider to a user at a client machine without trusting an internet service provider, wherein the content provider and internet service provider are different entities, said method comprising:

a. generating a first key known ~~only~~ to said content provider and not known to said user;

b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password;

c. transmitting said encrypted second key to the client machine;

~~c.~~ d. storing said encrypted second key on the ~~a~~ client machine; and

when said user first desires to access said data:

~~d.~~ e. decrypting said ~~second~~ encrypted second key using said ~~first key~~ one-time password; and

~~e.~~ f. accessing said data by decrypting an encrypted version of said data at said client machine using said second key.

2. (original) A method as recited in claim 1, further comprising the step of transmitting the identity of said client machine to said content provider to authenticate that

said user is using said client machine, thereby permitting said data to be accessed only on said client machine.

3. (original) A method as recited in claim 1, wherein said one-time password is a unique user identifier and wherein said one-time password is transmitted out of band.

4. (original) A method as recited in claim 1, wherein said second key is required in an algorithm that generates a session key which is used to decrypt said data.

5. (currently amended) A method for securely providing data of a content provider through an internet service provider to a user at a client machine without trusting an internet service provider, wherein said content provider and said internet service provider are different entities, said method comprising:

a. when said user accesses a web page of said content provider, downloading an applet from said content provider to said client machine;

b. generating a first key known ~~only~~ to said content provider and not known to said user;

~~b.~~ c. encrypting a second key using said first key and an encryption algorithm requiring a one-time password ~~and a separate user-provided password~~;

~~c.~~ d. transmitting said second encrypted key for ~~storing~~ storage of said encrypted second key on a client machine; and

when said user first desires to access said data:

~~d.~~ e. said applet requesting said one-time password from said user and, based on correct entry of said one-time password, decrypting said second encrypted key ~~using said user provided password~~; and

~~e.~~ f. accessing said data by decrypting an encrypted version of said data at said client machine using said second key.

6. (original) A method as recited in claim 5, further comprising the step of transmitting the identity of said client machine to said content provider to authenticate that said user is using said client machine, thereby permitting said data to be accessed only on said client machine.

7. (original) A method as recited in claim 5, wherein said one-time password is a unique user identifier and wherein said one-time password is transmitted out of band.

8. (original) A method as recited in claim 5, wherein said second key is required in an algorithm that generates a session key which is used to decrypt said data.

9. (currently amended) In a communications network having at least a content provider node and a plurality of client machines, a method of authenticating a user at one client machine seeking access to secure data of said content provider, wherein said user accesses said content provider through an internet service provider and wherein said internet service provider and said content provider are different entities, said method comprising:

a. transmitting g^a and the identity of the user of said one client machine to said content provider node, wherein g and a are random numbers and where a is known only to said client machine and is not known by said content provider, and where g is known to both content provider and said client machine;

b. generating g^b, where b is known ~~only~~ to said content provider node and is not known to said user;

c. encrypting g^b with a one-time password of said user;

d. calculating g^(a*b) by said client machine using said one-time password to decrypt said encrypted g^b; and

e. transmitting g^(a*b) to said content provider, whereby said client machine's knowledge of g^(a*b) authenticates said user to said content provider, wherein an encryption key K_{ab} for encrypting data to be transmitted from said content provider to said client machine and for decrypting the encrypted data at said client machine uses

g^(a*b).

10. (original) A method as recited in claim 9, further comprising the step of transmitting the identity of a particular one of said client machines to said content provider to authenticate that said user is using said client machine, thereby permitting said data to be accessed only on said client machine.

11. (original) A method as recited in claim 9, further comprising the step of performing a method authenticated code on g^(a*b) at said content provider and transmitting the results of performing said method authenticated code to said client, where said client machine verifies said results to authenticate said content provider.

12. (currently amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for securely providing data of a content provider to a user at a client machine, wherein data is transmitted to said user from said content provider through an internet service provider and wherein said content provider and internet service provider are different entities, said method comprising:

a. generating a first key known ~~only~~ to said content provider and not known to said user;

b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password; ~~and~~

c. transmitting said encrypted second key to the client machine;

~~c.~~ d. storing said encrypted second key on the ~~a~~ client machine; and

when said user desires to first access said data:

said second encrypted key is decrypted using said ~~first key~~ one-time password; and

said data is accessed by decrypting an encrypted version of said data at said client machine using said second key.

13. (currently amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for securely providing data of a content provider to a user at a client machine, wherein data is transmitted to said user from said content provider through an internet service provider and wherein said content provider and internet service provider are different entities, said method comprising:

a. when said user accesses a web page of said content provider, downloading an applet from said content provider to said client machine;

b. generating a first key known ~~only~~ to said content provider and not known to said user;

~~b.~~ c. encrypting a second key using said first key and an encryption algorithm requiring a one-time password ~~and a separate user-provided password~~; and

~~c.~~ d. transmitting said second encrypted key for ~~storing~~ storage of said encrypted second key on a client machine;

wherein, when said user first desires to access said data:

said applet requesting said one-time password from said user and, based on correct entry of said one-time password, decrypting said second encrypted key ~~is decrypted using said user-provided password~~; and

said data is accessed by decrypting an encrypted version of said data at said client machine using said second key.

14. (currently amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps in a communications network having at least a content provider node and a plurality of client machines, said method steps

authenticating a user of one client machine seeking access to secure data of said content provider, wherein data is transmitted to said user from said content provider through an internet service provider and wherein said content provider and internet service provider are different entities,, said method steps comprising:

a. transmitting g^a and the identity of the user of said one client machine to said content provider node, wherein g and a are random numbers and where a is known only to said client machine, and where g is known to both content provider and said client machine;

b. generating g^b, where b is known ~~only~~ to said content provider node and is not known to said user;

c. encrypting g^b with a one-time password of said user;

d. calculating g^(a*b) by said client machine using said one-time password to decrypt said encrypted g^b; and

e. transmitting g^(a*b) to said content provider, whereby said client machine's knowledge of g^(a*b) authenticates said user to said content provider, wherein an encryption key K_{ab} for encrypting data to be transmitted from said content provider to said client machine and for decrypting the encrypted data at said client machine uses g^(a*b).

15. (currently amended) A computer program product for securely providing data of a content provider to a user at a client machine without first trusting an internet service provider, wherein data is transmitted to said user from said content provider through an internet service provider and wherein said content provider and internet service provider are different entities, said computer program product comprising:

a. first instruction means for generating a first key known ~~only~~ to said content provider and not known to said user;

b. second instruction means for encrypting a second key using said first key and an encryption algorithm requiring a one-time password; ~~and~~

c. third instruction means for transmitting said encrypted second key to the client machine for storage of ~~storing~~ said encrypted second key on the ~~a~~ client machine;

when said user desires to first access said data:

said second encrypted key is decrypted using said ~~first key~~ one-time password; and

said data is accessed by decrypting an encrypted version of said data at said client machine using said second key.

16. (currently amended) A computer program product for securely providing data of a content provider to a user at a

client machine without trusting an internet service provider, wherein data is transmitted to said user from said content provider through an internet service provider and wherein said content provider and internet service provider are different entities, said computer program product comprising:

a. first instruction means for downloading an applet from said content provider to said client machine upon user access to a content provider web page;

b. second instruction means for generating a first key known ~~only~~ to said content provider and not known to said user;

~~b. second~~ c. third instruction means for encrypting a second key using said first key and an encryption algorithm requiring a one-time password ~~and a separate user provided password~~; and

~~c. third~~ d. fourth instruction means for transmitting said encrypted second key to said client machine for storage of ~~storing~~ said encrypted second key on a client machine;

wherein when said user first desires to access said data:

said applet requests said one-time password from said user and, based on correct entry of said one-time password, said second encrypted key is decrypted ~~using said user provided password~~; and

said data is accessed by decrypting an encrypted version of said data at said client machine using said second key.

17. (currently amended) A computer program product for use in a communications network having at least a content provider node and a plurality of client machines, said computer program for authenticating a user at one client machine seeking access to secure data of said content provider, wherein data is transmitted to said user from said content provider through an internet service provider and wherein said content provider and internet service provider are different entities, said computer program product comprising:

a. transmitting g^a and the identity of the user of said one client machine to said content provider node, wherein g and a are random numbers and where a is known only to said client machine, and where g is known to both content provider and said client machine;

b. generating g^b, where b is known ~~only~~ to said content provider node and not known to said user;

c. encrypting g^b with a one-time password of said user;

d. calculating g^(a*b) by said client machine using said one-time password to decrypt said encrypted g^b; and

e. transmitting g^(a*b) to said content provider, whereby said client machine's knowledge of g^(a*b) authenticates said user to said content provider, wherein an encryption key K_{ab} for encrypting data to be transmitted from said content provider to said client machine and for decrypting the encrypted data at said client machine uses g^(a*b).

18. (new) The method as recited in claim 2, wherein said content provider stores a mapping between said user and said client machine and wherein, when said user subsequently seeks to access additional data from said content provider, said method further comprises the steps of:

authenticating the user to said content provider based on said stored mapping;

generating a new encryption key based on said second key;

encrypting said additional data with said new encryption key;

transmitting said encrypted additional data to said client machine whereat the new encryption key is decrypted using said second key and said encrypted additional data is decrypted using said new encryption key.

19. (new) The method as recited in claim 6, wherein said content provider stores a mapping between said user and said

client machine and wherein, when said user subsequently seeks to access additional data from said content provider, said method further comprises the steps of:

authenticating the user to said content provider based on said stored mapping;

generating a new encryption key based on said second key;

encrypting said additional data with said new encryption key;

transmitting said encrypted additional data to said client machine whereat the new encryption key is decrypted using said second key and said encrypted additional data is decrypted using said new encryption key.

20. (new) The method as recited in claim 10, wherein said content provider stores a mapping between said user and said client machine and wherein, when said user subsequently seeks to access additional data from said content provider, said method further comprises the steps of:

authenticating the user to said content provider based on said stored mapping;

generating a new encryption key based on g^(a*b);

encrypting said additional data with said new encryption key;

transmitting said encrypted additional data to said client machine whereat the new encryption key is decrypted

using g^(a*b) and said encrypted additional data is decrypted using said new encryption key.